

Chapter I The Big Picture: Security Concepts and Operational Issues

Most schools in the United States are safe institutions, with disciplinary issues creating most disruptions. However, because of the 1998 campus slayings involving students, firearms, and multiple victims, schools and school programs are working harder to reach out to students, to teach them to be good citizens, to identify potentially dangerous personalities, and to develop appropriate intervention strategies. There are many excellent programs around the country that address the issues of bullying, anger, hate, abuse, drugs, alcohol, gangs, lack of role models, vandalism, and so forth. It is of great importance to the United States that these programs be pursued expeditiously. Unfortunately, these programs cannot be successful overnight (indeed, many must be initiated early in a child's life in order to be most effective) and do not yet exist in all schools. Meanwhile, security incidents are occurring in schools that must be dealt with now—perpetrators must be caught and consequences must be administered. School administrators would like to discourage security infractions by means of any deterrent available to them. One such approach sought more often today involves security technologies.

Security technologies are not the answer to all school security problems. However, many security products (e.g., cameras, sensors, and so forth) can be excellent tools if applied appropriately. They can provide school administrators or security officials with information that would not otherwise be available, free up manpower for more appropriate work, or be used to perform mundane tasks. Sometimes they can save a school money (compared to the long-term cost of per-

sonnel or the cost impact of not preventing a particular incident). Too often, though, these technologies are not applied appropriately in schools, are expected to do more than they are capable of, or are not well maintained after initial installation. In these cases, technologies are certainly not cost effective.

Why security technologies?

To reduce problems of crime or violence in schools: (1) the opportunities for security infractions should be eliminated or made more difficult to accomplish, (2) the likelihood of being caught must be greatly increased, and (3) consequences must be established and enforced. Item 3 is a social and political issue and needs to be addressed head on by school boards and communities across the country. This guide addresses only items 1 and 2.

Simply providing more adults, especially parents, in schools will reduce the opportunities for security infractions and increase the likelihood of being caught. However, adding dedicated professional security staff to perform very routine security functions has many limitations:

- Locating qualified people may be difficult.
- Humans do not do mundane tasks well.
- Manpower costs are always increasing.
- Turnover of security personnel can be detrimental to a security program.
- As in other security environments, more repetitious tasks become boring.

Hence, the possible role of security technologies expands. Through technology, a school can introduce ways to collect information or enforce procedures and rules that it would not be able to afford or rely on security personnel to do.

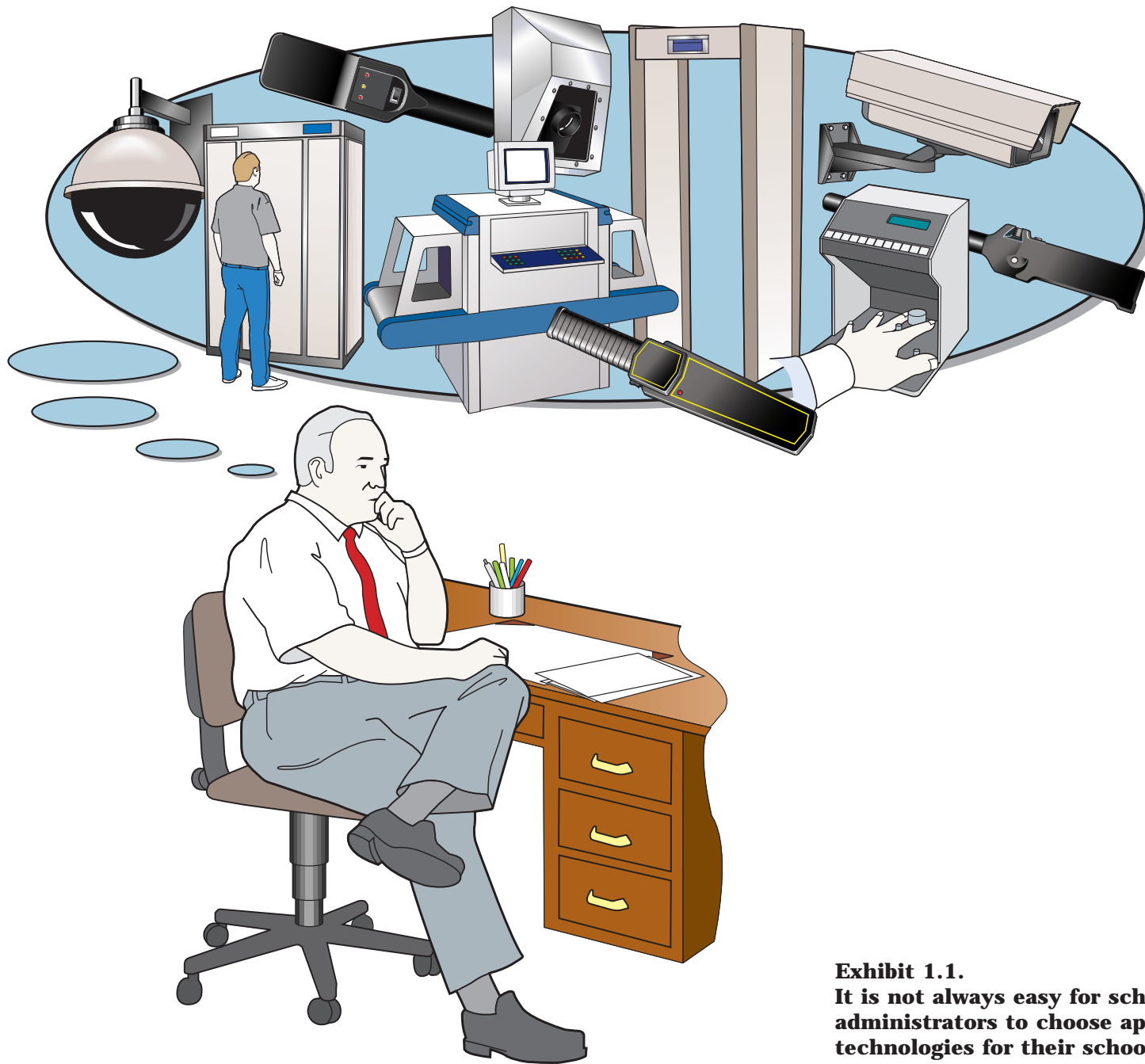


Exhibit 1.1.
It is not always easy for school administrators to choose appropriate technologies for their school.

Why security technologies have not been embraced by schools in the past

Anyone working in the security field is aware that there are thousands of security products on the market. Some of them are excellent, but many claim to be “the very best of its kind.” And, unfortunately, there are a significant number of customers in the country who have been less than pleased with the ultimate cost, maintenance requirements, and effectiveness of security technologies they have purchased. Schools have been no exception to this and have a few inherent problems of their own:

- Schools do not usually have the funding for aggressive and complete security programs.
- Schools generally lack the ability to procure effective security technology products and services at the lowest bid.
- Many school security programs cannot afford to hire well-trained security personnel.

- School administrators and their staff rarely have training or experience in security technologies.
- Schools have no infrastructures in place for maintaining or upgrading security devices—when something breaks, it is often difficult to have it repaired or replaced.
- Issues of privacy and potential civil rights lawsuits may prohibit or complicate the use of some technologies.

The issues come down to applying security technologies in schools that are effective, affordable, and politically acceptable but still useful within these difficult constraints.

Effectiveness versus affordability versus acceptability

Effectiveness, affordability, and acceptability are difficult tradeoffs and, occasionally, a seemingly ineffective solution to a security problem is chosen because of a lack of funding or pressure from the community to do something.

Arguments often used against security initiatives:

- “We’ve never done it that way before.”
- “This is a knee-jerk reaction.”
- “Our school will look like a prison.”
- “Students’ rights may be infringed upon.”
- “People will think we have a bad school,”
- “We may be sued.”

Some counter-arguments:

- “We need to evolve our security strategies to keep up with the changing times.”
- “This solution will take care of the immediate threat while longer term social programs are put into place.”
- “Our school will look like it is well controlled.”
- “Students have a right to a safe and secure school environment.”
- “We will gain a reputation for controlling our problems.”
- “We may be sued if we don’t take this action.”

Although many effective security measures are too expensive for schools, cost alone is not often the ultimate driver. Most major changes to security policies, including the introduction of technologies, are often brought on not by foresight but as a response to some undesirable incident.

This is not to say that a good argument should be made for applying every physical security approach in every school. “Appropriate” preparation is, by far, the greater “art” in security system design, and it includes an evolving plan, beginning with defining a particular school’s risks.

A systematic approach to identifying the security risks at a school

Note: The following discussion considers all security risks to schools—violence, drugs, theft, and vandalism—not just those that may be addressed by the technologies covered in this volume. Depending on the acceptance and demand for this guide, future additional volumes will address the remaining technologies in greater detail.

In the past, schools have rarely understood the need or had the time or resources to consider their security plans from a systems perspective—looking at the big picture of what they are trying to achieve in order to arrive at the optimal security strategy. A school’s security staff must understand what it is trying to protect (people and/or high-value assets), who it is trying to protect against (the threats), and the general environment and constraints that it must work within—the characterization of the facility. This understanding will allow a school to define its greatest and/or most likely risks so that its security strategy consciously addresses those risks. This strategy will likely include some combination of technologies, personnel, and procedures that do the best possible job of solving the

school’s problems within its financial, logistical, and political constraints.

Why is this careful identification of risk important? Because few facilities, especially schools, can afford a security program that protects against all possible incidents.

No two schools are alike and, therefore, there is no single approach to security that will work ideally for all schools. From year to year, even, a school’s security strategy will need revision because the world around it and the people inside it will always be changing.

Defining a school’s assets. For this school year, what is most at risk? The protection of the students and staff is always at the top of this list, but the measures taken to protect them will usually be driven by the defined threats. Are the instruments in the band hall very attractive targets for theft or vandalism? Is the new computer lab full of the best and most easily resold computers? Though desirable, a school cannot possibly afford to protect everything to the same level of confidence.

Defining a school’s threats. For this school year, who or what is your school threatened by? Gang rivalries? Fights behind the gym? Drugs hidden in lockers? Guns brought to school? Outsiders on campus? Drinking at lunchtime? Vehicle breakins? Graffiti in the bathrooms? Accidents in the parking lot? How sophisticated (knowledgeable of their task of malevolence) or motivated (willing to risk being caught or injured) do the perpetrators seem to be? Measures taken to protect against these threats are driven by the characterization of the facility and its surroundings as mentioned earlier.

Characterizing a school's environment. Any security strategy must incorporate the constraints of the facility so that all strengths, weaknesses, and idiosyncrasies are realized and provided for. How risks are approached will largely be driven by facility constraints. If theft and vandalism are primary risks for your school, answers to questions regarding the physical plant will determine the optimal security measures. Is the school new or old? Are the windows particularly vulnerable? Does everyone who ever worked at the school still have keys? What is the nighttime lighting like? Does the interior intrusion sensor system work well, or do the local police ignore the alarms due to a high false-alarm rate? Are visitors forced or merely requested to go through the front office before accessing the rest of the school?

If outsiders on campus are a primary concern, it will be necessary to recognize the facility's ability to control unauthorized access. How many entry points are there into the buildings? Are gangs present in the area? Are the school grounds open and accessible to anyone, or do fences or buildings restrict access (exhibit 1.2)? Is there easy access to the school roof? Where are hiding places within the building or on the premises? Is the student population small enough so that most of the staff would recognize most of the students and parents?

If issues of violence are a major concern, a thorough understanding of employees, student profiles, and neighborhood characteristics will be necessary. What is the crime rate in the neighborhood? Is the school administration well liked by the students? Are teachers allowed access to the school at night? Are students allowed off campus at lunch time? How much spending money do students generally have? Are popular hangouts for young people close by and, for business establishments, does management collaborate with the school? Are expelled

or suspended students sent home or to an alternative school? How many incidents of violence have occurred at the school over the past 4 years? What is the general reputation of the school, and how does it appear to an outsider? Are your most vocal parents prosecurity or proprivacy? Do your students like and respect your security personnel well enough to pass them pieces of information regarding security concerns? Once the school's threats, assets, and environmental constraints are understood, the security needs can be prioritized such that the school's security goals are understood by all those involved.

Identifying security needs and then securing the funding to pay for them are usually unrelated at most schools. Schools have to have a "Plan B," for program design which may be the perfect "Plan A"—but spread out over several years of implementation. If the desirable strategies (e.g., fencing, sensors, locker searches, speed bumps) are too costly or unpalatable to the community, a school may then need to modify the facility constraints (e.g., back entrances locked from the outside, no open campus for students, no teacher access after 10 p.m., all computer equipment bolted down, no lockers for students, and so forth).

Most school districts or school boards will be more supportive of security measures and the requested funding if they are well educated about the most likely risks faced each year and the options available. A security staff should not have the wide-open charter to "keep everything and everybody safe." A school board should be briefed as often as once a month as to what the current security goals are and what strategies are recommended, realizing that these will and must continue to evolve. If a school board member is clearly aware of a school's most important concerns and what



Exhibit 1.2. A 3-foot fence added very little security to this school that was constantly being vandalized.

is required to achieve them, then he or she is less likely to be swayed by an irate parent into making a decision that will handicap reasonable security efforts.

Designing the school security system

After identifying the risks or concerns at a noneducational facility, a methodical approach to the security plan would then examine possible solutions to each area of vulnerability from the perspective of:

Detection \longrightarrow *Delay* \longrightarrow *Response*

For any problem, it is necessary first to detect that an incident or problem is occurring. For example, when someone is breaking into a building, it is necessary that this act be detected and that information be supplied to the authorities as soon as possible. Next, this adversary must be delayed as long as possible so that the response force may arrive. A simple example of delay would be firmly bolting computer components onto large heavy desks, so that a thief is forced to use more time removing the bolts. Finally, someone, such as the police, must respond to the incident to catch the thief redhanded.

For a school environment, it is probably more appropriate to expand this model:

Deterrence \longrightarrow *Detection* \longrightarrow *Delay* \longrightarrow
Response/Investigation \longrightarrow *Consequences*

See exhibit 1.3 for more detail.

The most appealing step in any school security system should be to convince the perpetrator that he or she should not do whatever it is he or she is considering, whether the action is perceived as too difficult, not worthwhile, or the chances of being caught are quite

high. Clearly, most security measures employed in facilities are intended for the precise purpose of deterrence, whether it be to discourage a thief, a drug dealer, or an errant employee. (Note: Deterrence is not generally considered part of the security strategy for most high-risk government facilities; this is due in part to the fact that quite a bit of deterrence comes “free” with other security measures, and it would be difficult to attribute a lack of security problems to any particular deterrence effort.)

Unlike other facilities, where a perpetrator would be handed over to the authorities, and the consequences determined by law, a school often has the authority and/or opportunity to establish the consequences for incidents that occur on their campus. It is imperative, however, that schools do not assume authority that they do not have. Issues governed by law must be reported to the appropriate authority.

To illustrate the application of this model, consider the problem of nighttime breakins and theft in a school building. A model for the security strategy to address this might be:

Deterrence Close off the parking lot or driveways to vehicle traffic at night. Post signs that video cameras are in use on the campus (but only if you actually do have cameras). Use fencing strategically, but where fencing would be unacceptable, consider a barrier of thorny pyracantha bushes (exhibit 1.4). Allow a law enforcement officer to live on campus.

Detection	Install an intrusion detection system in all school hallways, administrative offices, and rooms with high-value
-----------	---

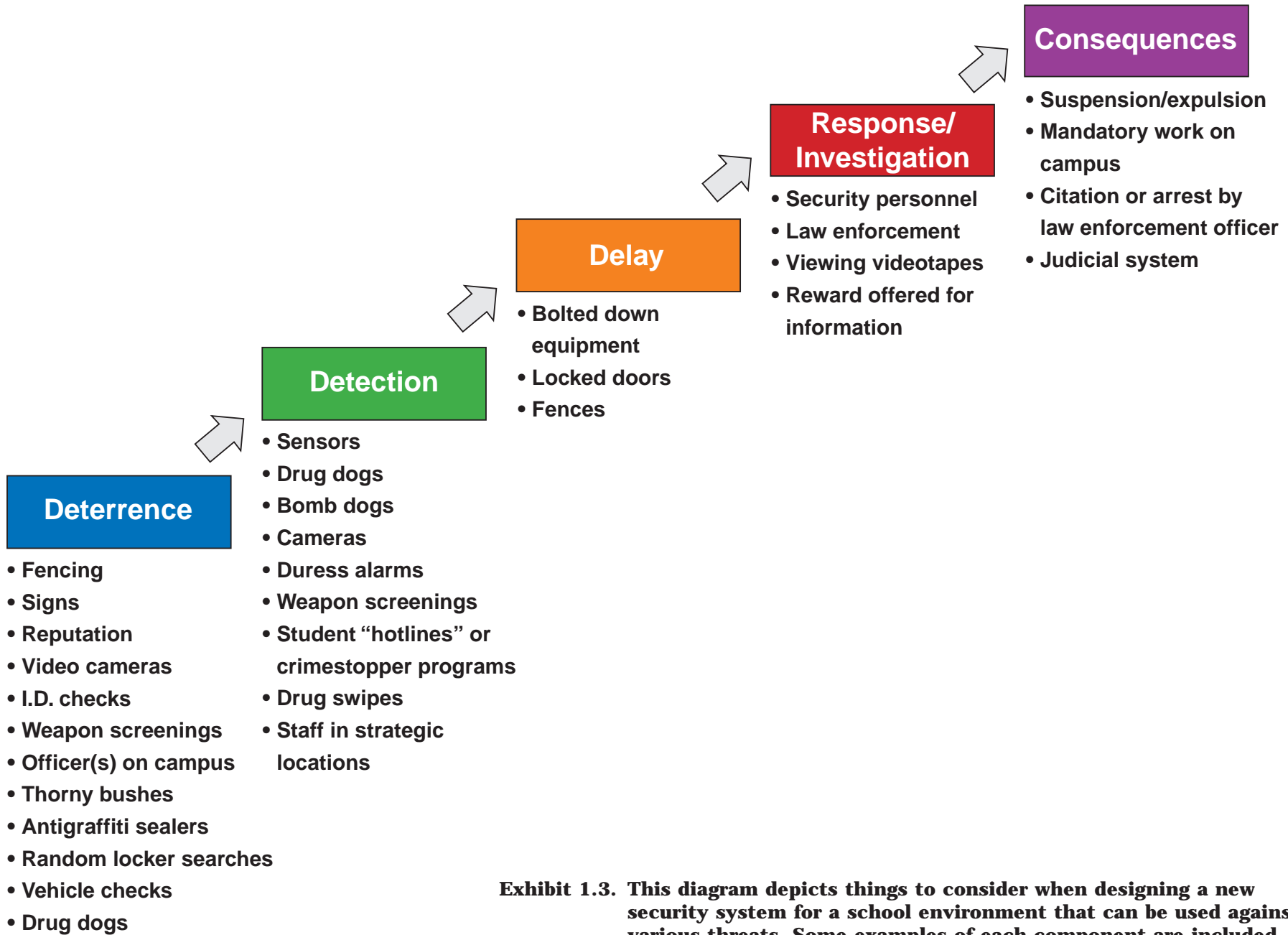




Exhibit 1.4. Pyracantha bushes can create an intimidating barrier where fences might be inappropriate. Caution may be advisable as to the location of bushes so that convenient hiding places for contraband are not created.

assets. Use motion sensors, magnetic switches on doors, heat sensors, and/or glass-break sensors as appropriate. Send alarm signals to the police, the officer on campus, and the school principal.

Delay	Bolt computers and TVs to desks and walls so that removing them is difficult and time consuming.
Response/ Investigation	Police and/or campus security arrives on the scene, makes arrests.
Consequences	Enforce consequences where possible and the school has the authority to do so. (This becomes an additional deterrent for the future, especially if nonsensitive pieces of information regarding the incident are released to staff, students, and the community.)

Schools do not normally have the opportunity for real-time detection and real-time response to security incidents; after-the-fact investigation is normally the best a school can hope for.

Although this model may not be appropriate for all aspects of security at a school, it can serve as a methodology for consideration. Its use can prevent some less-thought-out strategies. A true example of this is a large urban high school that was planning to purchase \$100,000 worth of exterior cameras to combat nighttime vandalism being inflicted on the exterior of the building. This plan was halted abruptly when the school was asked who would be available to watch the monitors from the 40-plus cameras (detection) and who would be able to respond quickly enough to these sporadic and relatively small incidents (response). A better and cheap-

er alternate plan was devised that included using anti-graffiti sealer on all brick surfaces, some strategically located wrought iron fencing that could not easily be climbed, and the replacement of a few particularly vulnerable windows with glass block.

A spectrum of physical security approaches

It will be assumed that consequences for undesirable actions have been put into place at a school; otherwise, there is little or no deterrence to be gained from any physical security measures designed to detect, delay, and respond to an incident. A wide array of security measures involving people, campus modifications, and/or technologies can be considered for most concerns, keeping in mind the unique characteristics of each school. A recurring message from school administrators is that the majority of their problems are brought onto campus by outsiders or expelled/suspended students so measures to keep outsiders off campus will generally be of global benefit. (Although this is not the case in all incidents, school administrators quite often find it more palatable to parents if security measures are justified based on the exterior threat rather than the suspicion of their children.) The following is a partial list of possible security measures to address various security issues:

(Most of the following suggested security measures are in use in one or more U.S. schools, but a few may not yet have been attempted. In any case, there is no comprehensive body of knowledge regarding their effectiveness. More research is needed to get a national picture on particular technologies. Also keep in mind that a school should always contact its legal counsel before participating in any new security program that involves searching or testing of people or property.)